Are cyber-blackouts in service networks likely?: Implications for Aggregate Cyber Risk Management

Pal, Ranjan

University of Cambridge

2018-10

Pal , R , Psounis , K , Kumar , A , Crowcroft , J , Hui , P , Golubchik , L , Kelly , J , Chatterjee , A & Tarkoma , S 2018 ' Are cyber-blackouts in service networks likely?: Implications for Aggregate Cyber Risk Management ' Techical Report , no. 926 , University of Cambridge . < https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-926.html >

http://hdl.handle.net/10138/311776

unspecified
publishedVersion

Technical Report

UCAM-CL-TR-926
ISSN 1476-2986

Number 926

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

Are cyber-blackouts in service networks likely?: implications for cyber risk management

Ranjan Pal, Konstantinos Psounis,
Abhishek Kumar, Jon Crowcroft, Pan Hui,
Leana Golubchik, John Kelly,
Aritra Chatterjee, Sasu Tarkoma

October 2018

15 JJ Thomson Avenue
Cambridge CB3 0FD
United Kingdom
phone +44 1223 763500

https://www.cl.cam.ac.uk/

Technical reports published by the University of Cambridge
Computer Laboratory are freely available via the Internet:

https://www.cl.cam.ac.uk/techreports/

ISSN 1476-2986

Are Cyber-Blackouts in Service Networks Likely? Implications for Aggregate Cyber Risk Management

Ranjan Pal*, Konstantinos Psounis, Abhishek Kumar, Jon Crowcroft, Pan Hui, Leana Golubchik, John Kelly, Aritra Chatterjee, Sasu Tarkoma

Abstract

Service liability interconnections among networked IT and IoT driven service organizations create potential channels for cascading service disruptions due to modern cybercrimes such as DDoS, APT, and ransomware attacks. The very recent *Mirai* DDoS and *WannaCry* ransomware attacks serve as famous examples of cyber-incidents that have caused catastrophic service disruptions worth billions of dollars across organizations around the globe. A natural question that arises in this context is: *what is the likelihood of a cyber-blackout?*, where the latter term is defined as the probability that all (or a major subset of) organizations in a service chain become dysfunctional in a certain manner due to a cyber-attack at some or all points in the chain. The answer to this question has major implications to risk management businesses such as cyber-insurance when it comes to designing policies by risk-averse insurers for providing coverage to clients in the aftermath of such catastrophic network events. In this paper, we investigate this question in general as a function of service chain networks and different loss distribution types. We[1] show somewhat surprisingly (and discuss potential practical implications) that following a cyber-attack, the probability of a cyber-blackout and the increase in total service-related monetary losses across all organizations, due to the effect of (a) network interconnections, and (b) a wide range of loss distributions, are *mostly* very small, regardless of the network structure - the primary rationale behind the results being attributed to degrees of heterogeneity in wealth base among organizations, and Increasing Failure Rate (IFR) property of loss distributions.

1 Introduction

Global commerce is undergoing a profound digital transformation. As it becomes increasingly electronic and IoT-driven, critical exposures in this sector are getting highly data-driven. As a result, the majority of modern business and economic risks are subsequently becoming cyber in nature. More importantly such cyber-risks are often networked and accumulate in a variety of different ways, thereby affecting many lines of business. As an example, commercial companies in diverse sectors such as automobiles, electronics, energy, finance, aerospace, etc., and their mutual trading relationships are characterized by systemic network linkages through major software providers (e.g., Oracle for DBMS

*Corresponding Author, Email: rp631@cam.ac.uk, rpal@usc.edu

[1]R. Pal and J. Crowcroft are with University of Cambridge, UK; K. Psounis and L. Golubchik are with University of Southern California, USA; A. Kumar and S. Tarkoma are with University of Helsinki, Finland; P. Hui is jointly with University of Helsinki, Finland and J. Kelly is Director of Analytics at QxBranch, USA; A. Chatterjee is Chief Underwriting Officer at Envelop Risk, Bermuda.

support). A cyber-attack (e.g., a zero day attack) motivated by a vulnerability in a software version can have a catastrophic cascading service disruption effect that might amount to net commercial losses worth billions of dollars across the various service sectors. As well-documented commercial cyber-attack examples in reality, the very recent *Mirai* DDoS (2016), *NotPetya* ransomware (2017), and *WannaCry* ransomware (2017) attacks caused havoc among firms in various industries (having trading relationships among them) across the globe, resulting in huge financial losses for the firms due to them being deemed dysfunctional in providing service to customers.

1.1 Research Motivation

In the wake of major targeted corporate cyber-attacks (e.g., attacks on Sony, Target) in the past half decade, risk mitigation has become a top board-level concern across many organizations worldwide. As a result, transfer based risk management products like cyber-insurance, which currently has a rapidly growing market (*Source* - Betterley Annual Report, 2015 [1], Advisen annual report 2016) is a major go-to solution for the current corporate sector worldwide, in the event of a cyber-attack. However, market surveys suggest that demand for cyber-insurance significantly exceeds the capacity currently provided by the insurance industry. The primary reason that most insurers give for being cautious about expanding capacity is the accumulation risk posed by cyber-threats. The main fear among insurers here is that cyber-threats are inherently scalable and systemic through their spread via network interconnectivity - a single malicious email generated by a botnet activity as part of a social engineering attack can result in an entire organization becoming dysfunctional with respect to the service it provides, and in turn potentially affecting business services of all other organizations that depend on it. In the event of cascading service disruptions due to a major cyber-attack, if all these organizations were to hold responsible their parent organization(s) on which they depend on for providing services, it is quite likely that the insurance company of a certain root organization would need to bear the responsibility of covering a huge aggregate/accumulated risk of all or multiple organizations in the service chain [2]. Shouldering this responsibility clearly may not be aligned with satisfying the budget constraints and profit requirements of most commercial risk-averse cyber-insurers, leave alone risk-tracking and risk-data availability challenges they might need to overcome to implement accumulative coverage policies [2].

Our Focus - Given a service chain network, our focus in this paper is to estimate the probability that *all* or a *major subset* of organizations (network nodes) in the network become dysfunctional in a certain manner (e.g., unable to provide cloud connectivity, inability to protect customer privacy, disruption of energy services) to provide service in the event of a cyber-attack, a situation which we define as a *cyber-blackout* [See Section 4.1 for details]. A robust estimate of the probability of a cyber-blackout is a necessary pre-requisite for considering the expansion of the service capacity of risk management products such as cyber-insurance. In scenarios of cascading cyber-risks, the probability value will act as a valuable input to cyber-insurance firms to allocate optimal portfolios among insurance and re-insurance investments. In addition, we will also investigate the practical implications of the likelihood and scale of cyber-blackouts on cyber-insurance ecosystems of today and the near future.

1.2 Research Contributions

We make the following research contributions in this paper.

- We design a graph-based model of service obligations, *GSOM*, between organiza-

tions in a service chain network. Our model specifies a set of nodes that represent service organizations together with the edges that represent service liability relationships between them. In the event of a cyber-attack, given the values of losses (either deterministic or stochastic) at the nodes in the network, GSOM computes via solving a fixed-point problem, the vector of service valuations that clears the network, and identifies the nodes in the chain that are dysfunctional to provide service. GSOM is very useful for analyzing how service-related losses propagate through an organizational service chain (see Section 3).

- Using GSOM, given the joint distribution of service-related losses across the network nodes (organizations) in the event of a cyber-attack, we analyze the probability of contagion that target organizations become dysfunctional due to a given organization somewhere in the network becoming dysfunctional. In this regard, we answer two important questions: (i) how likely it is that a given set of target organizations will become dysfunctional due to contagion from a *single source* organization, as compared to the likelihood that they become dysfunctional from direct losses to their own service-related assets that does not require dependency on other nodes?, and (ii) how much does the underlying network of service dependencies contribute to the *increase* in the probability of dysfunction of target nodes and corresponding expected value of losses, compared to a situation when there are no network links, i.e., each organization completely relies on its own resources to provide customer service?. Our analysis is very useful for analyzing the chance of a cyber-blackout event. As part of our results, we derive a general formula that surprisingly shows that the probability of a cyber-blackout is larger *mostly* in the absence of network connectivity than that in the presence of network connectivity, implying that simple network spillover effects have a limited impact with respect to service obligations between heterogeneous (in terms of monetary assets) organizations. We also show that network spillover effects are surprisingly small mostly under a wide range of joint distributions for plausible values of model parameters, regardless of the service dependency network topology. (see Section 4 for details) - the rationale behind these results being attributed to degrees of heterogeneity in organizational wealth, and the Increasing Failure Rate (IFR) property of loss distributions.

- We expand the set of cyber-attack sources from a single node to multiple nodes, and study the negative impact of simultaneous attacks on the entire network of organizations. Under a wide range of general loss distributions, we again surprisingly show that the increase in total (summed over all nodes in the organizational network) value of service-related losses due to network interconnections are mostly small, regardless of the network structure (see Section 5 for details).

2 Motivation Examples for Cyber-Blackout Study

In this section, we provide motivational background for our paper by describing various well known attack scenarios that are capable of launching a cyber-blackout, thereby potentially presenting an accumulative coverage setting for a cyber-insurance provider. We describe coverage accumulation scenarios for *six* key example processes [4] of cyber-loss in today's digital age. The examples highlight how correlated cyber-losses could impact a portfolio of cyber-insurance policies, and peep into the rationale of how a large number of accounts/organizations might suffer systemic losses from a single underlying cause.
Cyber Data Exfiltration - This process relates to the systemic release of confidential

customer records from many corporate enterprises (organizations). Some of the highest profile cyber-incidents (e.g., the *Sony*, *Target*, and *Equifax* cyber-incidents [4]) have been data breaches[2]: the loss of confidential data from organizations that breach the privacy of their customers, employees, clients, or counterparts. This has proved costly to the enterprise, resulting in notification costs, credit monitoring services, and compensation pay outs to all the individuals/organizations whose data was compromised, together with regulatory fines, response and forensic costs, and sometimes substantial litigation costs. The total accumulative losses to data breaches (both, first-party, and third-party losses faced from organizations in the service chain complaining of privacy breach of their data) faced by individual organizations have been instrumental in driving the expansion of the cyber-insurance market, as companies seek protection and risk partners in helping with response services.

Another burning example of cyber-data exfiltration might arise from the recently operative General Data Protection Regulation (GDPR) [8]. The key theme of GDPR, operative in the EU from May 25th, is that each of us owns our own data. Any company (EU local/EU multinational/companies worldwide operating with data of EU subjects including residents, citizens, and tourists) must therefore explicitly request permission to use any of our personal data, explaining why it would like to do so, and for how long. If we so agree, we can later withdraw our permission at any time. All of these rights must be provided to us by each company free of charge. One consequence is that each company must know, and (dynamically) document, what information (if any) they have about each individual. This may be a particular challenge for large, established corporations, since data about individuals may be spread across different business units and multiple databases, spreadsheets, off-site backup copies, or even paper archives, that would make synchronous dynamic updating of data difficult. Thus, will open up avenues for cyber-data exfiltration thereby leading to the aforementioned situation of accumulative losses due to a data breach.

Denial-of-Service Attack - This process relates to attacks that disable websites and disrupt online business activity across multiple organizations. Denial-of-Service (DoS) and Distributed DoS attacks are common methods of disrupting website business activities by bombarding them with traffic (e.g., the *Mirai* botnet-induced DDoS attack [9]). Half of all major U.S. organizations experienced a DoS attack on their websites in the past few years, and one in eight of those attacks overwhelmed website resilience and rendered Internet services unavailable (*Source* - SANS Institute). In April 2007, following a diplomatic row with Russia over a Soviet war memorial, Estonia was subject to DDos attacks which caused temporary shut down of infrastructure including everything from online banking and mobile phone networks to government services and access to health care information [16]. For a given organization, the cost of the business interruption caused by a DDoS attack of any particular duration is determined by the Internet dependency of the insured company i.e., the amount of revenue that would be lost per hour of Internet failure or connectivity loss. The capture of this information makes it possible to assess the accumulative loss of revenue that a given insured organization may be liable for (due to organizational dependencies in a service chain), from the potential for Internet outage in general. As another line of recent target applications for DDoS attacks is the catastrophic disruption of critical infrastructure services in the electricity, manufacturing, and transportation sectors by APT-driven DDoS attack vectors. A well known instance of such an attack type led to a series of power blackouts in Ukraine [10] in the last few years that caused

[2]Types of data include personal identity information (PII), payment and credit card information (PCI), protected health information (PHI), commercial confidential information (CCI), and intellectual property (IP).

significant damage to people's life and business activities. Such scenarios are also subject to accumulative coverage settings for cyber-insurers.

Cloud Service Provider Failure - This process relates to the scenario when large number of organizations have business operations disrupted by losing cloud-based functionality in the event of a major cloud service provider (CSP) suffering a service disruption due to a cyber-attack. The digital economy is increasingly dependent on cloud services and a rapidly growing number of companies make use of a CSP by outsourcing elements of their data storage, analytics, and information technology functions. If a CSP were to fail (e.g., *AWS* outage (2011), *Gmail* outage (2010), *Microsoft Sidekick* outage (2009) [4]) then their customers would suffer business losses, and hold the CSP liable for the loss. A CSP failure could also be the source of the exfiltration of confidential data records, or claims for data and software loss if data files were irrevocably deleted. This provides an accumulation issue for cyber-insurance where there is potential for a large number of organizations (and their subsequent business clients in a service chain) to make a claim for business interruption if a major provider of cloud services were to have a lengthy outage or failure, from any cause. The systemic dimension of cyber-risk concerns the triggering of large numbers of claims from companies that are CSP customers. The customers and their insurers may attempt to recover their loss payouts from the CSP (and possibly the insurer of the CSP).

Compromise of Financial Transactions - This process relates to theft of large sums in cyber-attacks on multiple enterprises (organizations) that carry out financial transactions. Insurers offer coverage to the financial services sector to cover losses that they might suffer from cyber-attacks, or computer based fraud, theft, or disruption occurring from compromising payment systems or technologies for managing financial transactions. Criminals have always targeted the money held in financial institutions, and physical bank robbery has given way to cybercrime as the preferred technique (e.g., *Carbanak APT Attack* (2013-2015), *Drinkman and Kalinin Attack* (2013) [4]). Although very large numbers of companies of all different types carry out financial transactions, ranging from retail to e-commerce, the transaction systems that carry the financial flows are the specific liabilities of financial transaction companies. The potential for widespread and systemic claims across all the different sectors of the economy from subverting payments after the point of sale are constrained by the legal liabilities being confined to the financial services companies operating the payment transfers. Thus, transaction risk is mostly aggregated in banking and payment management companies, and investment management systems.

Cyber-Extortion Through Ransomware - This process relates to the event when many companies are held to ransom by payoff seeking hackers disabling IT functionality. Cyber extortion is a rapidly growing area of organized cybercrime using ransomware - malicious software that lock up data or disrupt business until companies make a payoff. This has been a common method of extorting individuals and small businesses for some years (e.g., *LA Children's Presbyterian Hospital Attack* (2016) [11], *Bitfinex Attack*(2017) [12]). Cyber criminals are increasingly scaling up their operations and using extortion more commonly against larger companies as they gain confidence and technical expertise. In 2017, UK hospitals effectively shut down and had to turn away non-emergency patients after *WannaCrypt* ransomware ransacked its networks [5]. In the same year, *Maersk*, the world's largest container shipping company, was hit by *NotPetya* ransomware attack [6]. Although ransomware that encrypts data and locks computers is the most common type of extortion, companies may also be asked to make payoffs to avert the threat of other cyber-attack types including denial-of-service attacks, data exfiltration breach, and sabotage to deny a company internet or cloud services. Insurance repayment for extortion is a common coverage in many standalone affirmative cyber liability products in the market, and around

three quarters of products offer this. Following from the previously mentioned process examples, accumulative risk is something a cyber-insurance company needs to deal with in the case of ransomware extortions.

Aggregate Losses due to Cyber-warfare - Highly untraceable acts of modern cyber-warfare or cyber-terrorism by nation states aimed to achieve political and corporate gains, can lead to aggregate losses incurred by organizations. On this note, as per a recent report by Bloomberg Businessweek [13], data center equipment run by Amazon Web Services and Apple may have been subject to surveillance from the Chinese government via a tiny and virtually undetectable microchip inserted during the equipment manufacturing process. These illicit microchips were capable of instructing the device in which they were embedded in, to communicate with unauthorized computers located elsewhere on the Internet and preparing the device's operating system to accept new code, and hence, enabling attackers to alter how the device functioned, however they wanted. As an example, attackers could use this to steal intellectual property (IP) of organizations and their service providing clients, resulting in a situation of aggregate information leak targeted at the host [14]. For the microchip case, Netflix (Entertainment), BBC (News Broadcasting), Capital One Financial Corporation (Finance), Twitter (Social Media), and various departments of the US government were clients of Amazon Web Services [23][24]. Similarly, Best Buy (Consumer Electronics), Verizon Communications (Telecommunications), AT & T (Telecommunications), Sprint (Telecommunications), T-Mobile U.S. (Telecommunications), were clients of Apple [17]. Here, Amazon, Apple may be held liable by their clients for IP loss damages inflicted during such attacks, thereby contributing to accumulative risk for a cyber-insurance company (includes self-insurance) to deal with.

Aggregated Risk in IoT-Driven Smart Cities - In the near future, people are likely to populate their homes, offices, and neighborhood with a dense network of potentially billions of tiny transmitters and receivers which have ad-hoc networking abilities. These IoT devices can directly communicate amongst themselves, creating a new unintended communication medium that completely bypasses the traditional norms of communications such as telephony and the Internet. In a recent work, Ronen et.al., [7] has successfully demonstrated that even though IoT devices might be manufactured by popular and reputed firms deploying industry-standard cryptographic techniques, they can be still misused by hackers to spread infectious malware from one IoT device to all physically adjacent neighbors, causing city-wide disruptions which are very difficult to stop and investigate [7]. In the case of "city" insurance agencies insuring their clients in the future, aggregate cascading risks due to unavailability of service is something they might have to deal with.

3 System Model

In this section, we propose our graph-based model of service obligations, GSOM, between organizations in a service chain network that will be used in this paper to investigate and analyze cyber-blackout probabilities.

3.1 Basic Ingredients of GSOM

GSOM has four basic ingredients: (i) a set of n nodes $N = \{1, 2, ..., n\}$ characterizing organizations, (ii) an $n \times n$ liability matrix $\bar{P} = (\bar{p}_{ij})$ where $\bar{p}_{ij} \geq 0$ is the payment *due* from node i to node j in the event of a claim made by j on i in the aftermath of a cyber-attack (e.g., an organization claiming that due to CSP failure, it incurred a business loss worth a certain monetary amount) with $\bar{p}_{ii} = 0$, (iii) $\vec{c} = (c_1, c_2, ..., c_n) \, \epsilon \, \mathrm{R}_+^n$, representing the vector of wealth/resource amount held by each node $i \in N$, that is not yet subject

to a cyber-attack, and (iv) $\vec{b} = (b_1, b_2, ..., b_n)\, \epsilon\, \mathrm{R}_+^n$, representing the vector of liability-free losses accrued by each node $i \in N$, in the aftermath of a cyber-attack. We make the general assumption in the paper that organizational claims, wealth, and losses can be expressed monetarily in the event of a cyber-attack. *Also note that the liability matrix embeds the service chain network.* For each node $i \in N$, the following relationship holds:

$$w_i = c_i + \sum_{j \neq i} \bar{p_{ji}} - \bar{p_i}, \tag{1}$$

where w_i is the net wealth of node i in the aftermath of a cyber-incident (given that the claim payouts are appropriately meted out), and is unrestricted in sign, and $\bar{p_i}$ is the net liability of i. A negative value of w_i denotes the inability of organization i to payout claims made by organizations liable on i. Observe that the net liability of i is expressed as

$$\bar{p_i} = b_i + \sum_{j \neq i} \bar{p}_{ij}.$$

Similarly, the net non-liability (assets) of organization i in the aftermath of a cyber-attack is given by $c_i + \sum_{j \neq i} \bar{p}_{ji}$.

3.2 GSOM for Post-Attack Scene

Having discussed the basic elements of GSOM, our primary goal here is to build GSOM to handle the case when resources that have not yet been hit by a cyber-attack are suddenly subject to a loss that might trigger service disruption in a service chain network.

Let the amount c_i for each node i be subject to a random shock or loss of value X_i in the event of a cyber-attack, where X_i is a random variable taking values in the interval $[0, c_i]$. Thus, in the aftermath of the attack, resource amount c_i for node i is reduced to $c_i - x_i$, where x_i is the instance of X_i. Let $F(x_1, x_2, ..., x_n)$ be the joint cumulative function of these losses, that is central to analyzing the process of the spread of "organizational dysfunctionality" due to cyber-attacks. We importantly note that a *necessary* (but not sufficient and complete) component to estimating or approximating $F()$ is the use of techniques like Monte Carlo simulation, percolation theory, or statistical mean field models, that popularly capture the spread of the infection (attack) vector (e.g., a virus, worm, bot) across a network, and is not the focus of our paper. The interested reader is referred to [18] [19] [20] [21] to get insights about some ways to mathematically evaluate this necessary component contributing to the value of $F()$. *In our work, we adopt a conservative (and hence more challenging) approach of assuming general continuous forms of $F()$ for the purpose of analysis*, without focussing our efforts (via the use of the aforementioned necessary component) on finding/assuming *specific* continuous forms of $F()$ that might be setting-dependent.

Define the relative liabilities matrix $A = (a_{ij})$ to be the $n \times n$ matrix with the entries:

$$a_{ij} = \begin{cases} \frac{\bar{p}_{ij}}{\bar{p}_i}, \text{ if } \bar{p}_i > 0 \\ 0, \text{if } \bar{p}_i = 0 \end{cases}$$

Thus, a_{ij} is the proportion of organization i's monetary obligations owed to organizations j in the aftermath of cyber-attack. Here, $a_{ij} \leq 1$ for each i and subsequently matrix A is substochastic.

Given a loss realization vector $\vec{x} = (x_1, ..., x_n) \geq 0$, *our aim is to evaluate a vector that corresponds to the payments that balance monetary assets and liabilities at each node (organization).* Based on the values in this vector, we will know whether an organization

Table 1: Table of Important Notations

N	set of organizations
$\bar{P} = (\bar{p}_{ij})$	payment matrix
$\overrightarrow{\mathrm{c}}$	vector of wealth held by each organization i
$\overrightarrow{\mathrm{b}}$	vector of liability-free losses
$\bar{P}_i$	net liability of i
X_i	random variable representing loss to i on random shock
$F(x_1, ...x_n)$	joint cdf of losses at organization
$A = (a_{ij})$	relative liability matrix
$\overrightarrow{\mathrm{P}}(\overrightarrow{\mathrm{x}})$	clearing vector
β_i	proportion of i's monetary liabilities to other nodes
λ_i	leverage ratio of organization i w.r.t. c_i
$\overrightarrow{\mathrm{S}}$	vector of monetary shortages at organizations

does have the ability to handle liabilities from other organizations in the service chain, in the event the latter hold the former liable for service disruptions due to a cyber-attack. In this paper, we term the vector as a *clearing vector* due to its relevance in balancing assets and liabilities. Mathematically, we represent the clearing vector as $\vec{p}(\vec{x}) = \{p_i(\vec{x})\}$; $\vec{p}(\vec{x}) \in \mathrm{R}_+^n$, and it is evaluated as the solution to the following fixed point equation:

$$p_i(\vec{x}) = \bar{p}_i \wedge \left(\sum_j p_j(\vec{x}) a_{ji} + c_i - x_i \right)_+, \tag{2}$$

where the structure $(\cdot)_+$ above indicates that if the value inside the parenthesis is less than zero, the value is zero. $\wedge$ denotes the min operator, where $\vec{x} \wedge \vec{y} = (\min[x_i, y_i], .., \min[x_n, y_n])$ The solution to this equation, for each node i, is evaluated under a *pro-rata* allocation mechanism, i.e., the amount of unresolved liabilities at node i (when its net assets are less than its net liability) is allocated in a proportional manner across its neighbors in the network induced by the liability matrix. A pro-rata allocation is a standard allocation mechanism in financial debt theory [3] [22], and we adopt this standard in our paper while allocating service liability debts. Given a solution to (2), an organization i is said to be *dysfunctional* if $p_i(\vec{x}) < \bar{p}_i(\vec{x})$ implying that its assets are less than the liability it owes to other organizations in the service chain network.

3.3 Uniqueness of the Clearing Vector

Here, we investigate on the uniqueness of clearing vector obtained as the solution to the fixed point equation in (2). In this regard, we have the following theorem.

Theorem 1. *The clearing vector is unique if from every organizational node i there exists a chain of positive obligations to some organizational node k that has positive obligations to itself.*

Proof. It follows from [3] that a solution to (2) can be constructed iteratively as follows. Given a vector $\vec{x}$, define the mapping $\Phi : \mathrm{R}_+^n \to \mathrm{R}_+^n$ as

$$\Phi_i(\vec{p}) = \bar{p}_i \wedge \left(\sum_j p_j a_{ji} + c_i - x_i \right)_+. \tag{3}$$

Starting with $\vec{p^0} = \bar{p}$, let $\vec{p^1} = \Phi(\vec{p^0})$, $\vec{p^2} = \Phi(\vec{p^1})$,..., and so on. This iteration yields a monotone decreasing sequence $\vec{p^0} \geq \vec{p^1} \geq$ ..... Since it is bounded below it has a limit p', and since Φ is continuous p' satisfies (2). Hence it is a clearing vector. We now claim that p' is in fact the only solution to (2). Suppose by way of contradiction that there is another clearing vector, say $p'' \neq p'$. Then, the net worth of all organizational nodes must be the same under the two vectors, i.e.,

$$p'A + (c - x) - p' = p''A + (c - x) - p''.$$

Rearranging the terms it follows that

$$(p'' - p')A = p'' - p'; \, p'' - p \neq 0.$$

This means that the matrix A has eigen value 1, which is impossible because under our assumption A has spectral radius less than 1 - equivalent to the condition that from every organizational node i there exists a chain of positive obligations to some organizational node k that has positive obligations to itself. Thus, p' is the only solution to (2) and equivalently the clearing vector is unique. ■.

Theorem Implication - The uniqueness of the clearing vector provides the benefit of practically dealing with a single vector of liability payments, over the challenge of computationally searching for multiple vectors. The assumption that matrix A has a spectral radius less than 1 is quite practical in the sense that a chain of obligations ending in an obligation loop around the same organization, i.e., self-liability, is common in practice. As an example, the concept of self-liability could arise in the context of the popular notion of self-insuring an organization, which is common in business sectors.

4 Estimating Blackout Chance - Single Source Case

In this section, we estimate the probability of a cyber-blackout among a given set of organization nodes due to a contagion/cascading effect, when a particular source node becomes dysfunctional to provide service in the aftermath of a cyber-attack. This section is divided into three main parts: in the first part we provide a non-trivial general estimate of cyber-blackout probability irrespective of the loss distribution function; in the second part we estimate the cyber-blackout probability for a certain popular family of loss distributions, i.e., the Beta distribution, and study the effect of the underlying service network topology on the estimate; finally we study the effect of various distributions on the estimate of cyber-blackout probability. A collection of important notations used in the paper is provided in Table I.

4.1 Analysis Setup

We first re-iterate the definition of the terms *organizational dysfunction* and *cyber-blackout*. As previously mentioned, organizational dysfunction happens when a given organization is unable to provide service to customers who rely on the former. Service could be of myriad forms, one popular example being the ability to protect customer private information; another example of a critical nature being the ability to provide non-interrupted energy to different customer segments in the industry. Potential impact of organizational dysfunction could result in monetary business losses, and loss of reputation resulting in loss of business. A cyber-blackout happens when individual organization dysfunction contributes to a cascade *(due to a contagion effect)* of organizational dysfunctions, where each subsequent organization that became dysfunctional was relying on other organizations that had

already become dysfunctional. Note here that an organization could be a single user as well. A practical example of a cyber-blackout is service disruption in a power grid caused by a cyber-attack which in turn causes a cascade of power unavailability issues in different sectors (e.g, manufacturing, transportation) of the industry, thereby leading to business disruptions that cause commercial losses. *In our work we characterize dysfunctionality in a monetary fashion by mapping it to the case when the monetary value of the available resources of an organization is less than what it owes other organizations (in the event of their unability to provide service) which are liable on the former for service.* More formally, given a solution to (2), an organization i is said to be *dysfunctional* if $p_i(\vec{x}) < \bar{p}_i(\vec{x})$ implying that its assets are less than the liability it owes to other organizations in the service chain network.

In order to formulate our results, we need the following notation. Let D be the set of nodes that we are interested in investigating whether they can go dysfunctional due to a cascading disruption effect resulting from a cyber-attack on a given source node i that made i dysfunctional. Let $\beta_i = \frac{\bar{p}_i}{b_i + \bar{p}_i}$ be the proportion of node i's service-related monetary liabilities to other organizational entities (nodes) in the system. We assume that $\beta_i > 0$, i.e., each node has a non-zero service liability external to itself. Recall that $w_i > 0$ is node i's initial net worth in the aftermath of it being subject to a cyber-incident, and c_i represents the vector of wealth/resources held by node i that is *not yet* subject to cyber-attack. *We assume that $w_i < c_i$, since otherwise i could never go dysfunctional directly through losses in c_i post a cyber-attack that affects c_i.* We define the ratio $\lambda_i = \frac{c_i}{w_i} \geq 1$ to be the leverage ratio of i with respect to c_i, and denotes the vulnerability of i - more the c_i, greater the potential of loss in c_i through a cyber-attack, leading to i being more vulnerable.

4.2 Estimate of Blackout Probability

In this section, given D and a node $i \notin D$, we first derive a general estimate of the cyber-blackout probability without taking into account specific forms of loss distribution functions. In this regard, we are interested in two quantities: *(i) a probability estimate that all organizations in D go dysfunctional, and (ii) the mathematical condition which guarantees the impossibility of a cascading effect from i to D.* The first quantity has implications to a cyber-insurer in the insurance industry who might be responsible for covering aggregate or accumulative risks of the organizations in D, and the value of this quantity will help the insurer design and manage its portfolio mechanisms to prevent it from going bankrupt. The second quantity has implications on individual organizations regarding boosting their investments in cyber-security so much as to prevent them getting dysfunctional and subsequently saving face and money, and furthermore arresting a cascading service disruption process.

We have the following proposition regarding a general *bound-based* estimate of the cyber-blackout probability independent of the specific forms of loss distribution functions.

Proposition 2. *Suppose that only organizational node i suffers a loss in its c_i from a cyber-attack, i.e., $x_j = 0, \forall j \neq i$, and that no organization is dysfunctional prior to i suffering the loss. Fix a set of nodes D not containing i. The probability that the loss causes all nodes in D to become dysfunctional is* ***upper bounded*** *by*

$$P\left(X_i \geq w_i + \frac{1}{\beta_i}\sum_{j \in D} w_j\right). \tag{4}$$

A cascading effect from i to D is impossible if

$$\sum_{j\in D}\frac{w_j}{w_i} > \beta_i(\lambda_i - 1). \tag{5}$$

Proof. Let $D(\vec{x}) \equiv \bar{D}$ be the dysfunctional set resulting from the loss vector X, whose coordinates are all zero except X_i. By assumption i causes other nodes to become dysfunctional, hence i itself must become dysfunctional, i.e., $i \in \bar{D}$. To prove (4), it suffices to show that

$$\beta_i(X_i - w_i) \geq \sum_{j\in\bar{D}-\{i\}} w_j \geq \sum_{j\in D} w_j. \tag{6}$$

The second inequality in (6) follows from the assumption that no nodes are in default before the loss and the fact that we must have $d \subseteq \bar{D} - \{i\}$ for all nodes in D to default. For the first inequality in (6), define the *shortage* at organizational node j to be the difference $s_j = \bar{p}_j - p_j$. From (2) we see that the vector of shortages $\vec{s}$ satisfies

$$\vec{s} = (\vec{s}A - w + X)_+ \wedge \bar{p}.$$

Using (3) we have $s_j > 0$ for $j \in \bar{D}$ and $s_j = 0$ otherwise. We use a subscript $\bar{D}$ as in $s_{\bar{D}}$ or $A_{\bar{D}}$ to restrict a vector or matrix to the entries corresponding to nodes in the set $\bar{D}$. Then the vector of shortages as the nodes of $\bar{D}$ satisfies

$$s_{\bar{D}} \leq s_{\bar{D}}A_{\bar{D}} - w_{\bar{D}} + X_{\bar{D}}, \tag{7}$$

hence

$$X_{\bar{D}} - w_{\bar{D}} \geq s_{\bar{D}}(I_{\bar{D}} - A_{\bar{D}}). \tag{8}$$

The vector $s_{\bar{D}}$ is strictly positive in every coordinate. From the definition of β_j we also know that the jth row sum of $I_{\bar{D}} - A_{\bar{D}}$ is at least $1 - \beta_j$. Hence,

$$s_{\bar{D}}(I_{\bar{D}} - A_{\bar{D}}) \cdot 1_{\bar{D}} \geq \sum_{j\in\bar{D}} s_j(1-\beta_j) \geq s_i(1-\beta_i). \tag{9}$$

From (7) it follows that the shortage at node i is at least as large as the initial amount by which i becomes dysfunctional, that is,

$$s_i \geq X_i - w_i > 0. \tag{10}$$

From (8) - (10) we can conclude that

$$\sum_{j\in\bar{D}}(X_j - w_j) \geq s_i(1-\beta_i) \geq (X_i - w_i)(1-\beta_i). \tag{11}$$

This establishes (6) and the first statement of the proposition. The second statement follows from the first by recalling that the loss to c_i's cannot exceed their value, i.e., $X_i < c_i$. Therefore, by (4) the probability of contagion in the context of organizational dysfunctionality is zero if

$$c_i \leq w_i + \frac{1}{\beta_i}\sum_{j\in D} w_j.$$

Dividing through by w_i we see that this is equivalent to the condition

$$\sum_{j\in D}\frac{w_j}{w_i} > \beta_i(\lambda_i - 1),$$

which is the second statement of the proposition. Hence we have proved Proposition 2. ■

Proposition Implication - Note that the bounds in the theorem are completely general and do not depend on the distribution of the losses, or on the network topology. The condition in (5) is intuitive and states that dysfunction contagion from i to D is impossible if the total net worth of the nodes in D is sufficiently large (could be made possible by making proper investments in cyber-security) relative to the net worth of i weighted by (a) the exposure of the system to organizational node i as measured by β_i, and (b) the vulnerability of i as measured by the leverage ratio λ_i. More generally contagion will be weak if unless originating node is highly leveraged and has a relative high proportion of obligations to other nodes (e.g., if originating node is an organization like Amazon providing cloud services to multiple other organizations [23][24]). A similar interpretation applies to (4).

Cyber-Insurance Perspective - In the context of cyber-insurance, the proposition implies that insurers should incentivize organizations (through appropriate contract design) to boost up their cyber-hygiene so that an organization's net worth is high. This has been a challenging problem in the cyber-insurance space, and one particular solution direction for networks has recently been explored by the authors in [25].

Contagion vs Independent Losses - We now investigate results tying the probability of a cyber-blackout through contagion from a given organizational node i to a given subset D of nodes, to the probability of the same under direct independent losses (e.g., losses incurred by organizations due to cyber-attacks that take advantage of poor cyber-hygiene practices in the organizations) experienced at the nodes. *We say that the contagion effect with respect to organizational node dysfunction is weak if*

$$P\left(X_i \geq w_i + \frac{1}{\beta_i}\sum_{j\in D} w_j\right) \leq P(X_i > w_i)\prod_{j\in D} P(X_j > w_j). \tag{12}$$

The expression on the left bounds the probability that nodes in D become dysfunctional through contagion from i, while the expression on the right is the probability (computed using the loss distribution for individual nodes) that the same nodes become dysfunctional through independent direct losses. The intuition for weak contagion is as follows: the RHS of the expression has the product of events, which means we consider the case where all nodes in D and node i get dysfunctional in an independent fashion. Thus, we have a sequence of 'less than 1' terms making the RHS smaller and smaller, yet it never gets small enough to become smaller than the LHS, that represents the network contagion effect. It goes without saying that the inequality depends heavily on w_i and β_i, and specific conditions in this regard are stated in the implications of Theorem 3 (see later). Note that in practice the assumption of direct independent losses is somewhat unrealistic: in practice one would expect the losses to different nodes be positively associated (correlated). In that case the probability of organizational dysfunction is even larger, and the above equation would hold here as well. *We say that the contagion effect is strong if*

$$P\left(X_i \geq w_i + \frac{1}{\beta_i}\sum_{j\in D} w_j\right) > P(X_i > w_i)\Pi_{j\in D} P(X_j > w_j). \tag{13}$$

The intuition for a strong contagion effect is just the converse of that for a weak contagion effect.

4.3 Distribution-Based Estimate of Cyber-Blackout Probability

Having provided a general estimate of the cyber-blackout probability, we now estimate this probability under the effect of a given loss distribution across different nodes in the organizational network. Let us assume that the cyber-losses at a given organizational node i scales with the portfolio c_i of the organization. Based on recent data from Symantec [26], this is a reasonable assumption to make irrespective of whether cyber-attackers target organizations big or small. Let us also assume that the distribution of these *relative losses*, i.e., with respect to c_i, is the same for the nodes, and *independent* among the nodes (note that this *does not* imply absolute losses are independent).

Then, there exists a distribution function $H : [0,1] \to [0,1]$ such that

$$F(x_1, ..., x_n) = \Pi_{1 \leq i \leq n} H\left(\frac{x_i}{c_i}\right). \tag{14}$$

Beta distributions provide a flexible standard family with which to model the distribution of relative losses that lie in the interval $[0,1]$, and generalizes other distributions that work with bounded intervals [27]. We work with *Beta densities* of the form

$$h_{p,q} = \frac{y^{p-1}(1-y)^{q-1}}{B(p,q)},\ 0 \leq y \leq 1,\ p,q \geq 1, \tag{15}$$

where $B(p,q)$ is a normalizing constant. Note that (15) is general enough to allow a mode anywhere in the unit interval. The subset with $p = 1$, $q > 1$ has a decreasing density and seems the most realistic, whereas the subset with $q = 1$, $p > 1$ has an increasing density and could be considered "heavy-tailed" in the sense that it assigns greater probability to greater losses. We have the following result regarding a distribution specific estimate of the cyber-blackout probability.

Theorem 3. *Assume relative loss distributions across all organizational nodes are i.i.d. Beta distributed, and the net worth of every node is initially non-negative. Let D be a non-empty subset of nodes and let $i \notin D$. Then a contagion effect with respect to organizational dysfunction is impossible if*

$$\sum_{j \in D} w_j > w_i \beta_i (\lambda_i - 1), \tag{16}$$

and is weak if

$$\sum_{j \in D} w_j \geq w_i \beta_i \sum_{j \in D} \frac{\lambda_i - 1}{\lambda_j}. \tag{17}$$

Proof. Proposition 2 implies that contagion is weak from i to D if

$$P\left(X_i \geq w_i + \frac{1}{\beta_i} \sum_{j \in D} w_j\right) \leq P(X_i > w_i) \Pi_{j \in D} P(X_j > w_j). \tag{18}$$

On the other hand this certainly holds if $w_i + \frac{1}{\beta_i} \sum_{j \in D} w_j > c_i$, for then contagion is impossible. In this case we obtain, as in (5)

$$\sum_{j \in D} \frac{w_j}{w_i} > \beta_i (\lambda_i - 1). \tag{19}$$

Suppose on the other hand that $\left(w_i + \frac{1}{\beta_i} \sum_{j \in D} w_j\right) \leq c_i$. By assumption the relative losses $\frac{X_k}{c_k}$ are independent and beta distributed as in (15). In the uniform case $p = q = 1$,

(18) is equivalent to

$$\left[1-\left(\frac{w_i}{c_i}+\frac{1}{\beta_i c_i}\right)\sum_{j\in D} w_j\right] \leq \left(1-\frac{w_i}{c_i}\right)\Pi_{j\in D}\left(1-\frac{w_j}{c_j}\right). \tag{20}$$

We claim that (20) implies (18) for the full family of Beta distributions in (16). To see why, first observe that the cumulative distribution $H_{p,q}$ of $h_{p,q}$ satisfies

$$1-H_{p,q}(y)=H_{q,p}(1-y).$$

Hence (18) holds if

$$H_{q,p}\left(1-\frac{w_i}{c_i}-\frac{1}{\beta_i c_i}\sum_{j\in D} w_j\right) \leq H_{q,p}\left(1-\frac{w_i}{c_i}\right)\Pi_{j\in D} H_{q,p}\left(1-\frac{w_j}{c_j}\right). \tag{21}$$

But (21) follows from (20) because Beta distributions with $p, q \geq 1$ have the submultiplicative property

$$H_{q,p}(xy) \leq H_{q,p}(x)H_{q,p}(y),\ x, y \in [0,1].$$

It therefore suffices to establish (21), which is equivalent to

$$\frac{1}{\beta_i c_i}\sum_{j\in D} w_j \geq \left(1-\frac{w_i}{c_i}\right)\left(1-\Pi_{j\in D}\left(1-\frac{w_j}{c_j}\right)\right). \tag{22}$$

Given any real number $\theta_j \in [0,1]$, we have the inequality

$$\Pi_j(1-\theta_j) \geq 1-\sum_j \theta_j. \tag{23}$$

Hence a sufficient condition for (22) to hold is that

$$\frac{1}{\beta_i c_i}\sum_{j\in D} w_j \geq \left(1-\frac{w_i}{c_i}\right)\sum_{j\in D}\frac{w_j}{c_j}). \tag{24}$$

After rearranging the terms and using the fact that $\lambda_k = \frac{c_k}{w_k}$ for all k, we obtain (17). This concludes the proof of Theorem 3. ■

From the argument in (21), it is evident that the same result holds if the losses to each node j are distributed with parameters p_j, q_j in (15) with $p_i \leq \min_{j\in D} p_j$ and $q_i \geq \max_{j\in D} q_j$.

Theorem Intuition - As noted in Proposition 2, the condition in (16) states that the contagion from i to D is impossible if the total net worth of the nodes in D is sufficiently large (could be made possible by making proper investments in cyber-security) relative to the net worth of i weighted by (a) the exposure of the system to organizational node i as measured by β_i, and (b) the vulnerability of i as measured by the leverage ratio λ_i. The condition in (17) compares the total net worth of D relative to that of i with the leverage ratio of i relative to that of the nodes in D. With other parameters held constant, increasing the relative net worth of D (again via making higher investments in security) makes contagion weaker in the sense that it strengthens the inequality; increasing the leverage ratio of i relative to that of the nodes in D has the opposite effect because there is higher potential to target unattacked resources worth c_i. Importantly, the two effects are mediated by β_i - a lower β_i makes D vulnerable to i and makes D less sensitive to the

degree of leverage at i. Now recalling that $\lambda_j = \frac{c_j}{w_j}$, we can write (17) in the following equivalent form:

$$\frac{\sum_{j\in D} c_j \lambda_j^{-1}}{\sum_{j\in D} \lambda_j^{-1}} \geq c_i \beta_i (1 - \lambda_i^{-1}). \tag{25}$$

Written this way, the condition states that contagion from i to D is weak if the average size of the nodes in D weighted by their inverse leverage ratios is sufficiently large relative to i - evident as a result of high net worth of nodes in D. On the right side of the inequality in (25), $c_i\beta_i$ measures the organizational system's exposure to node i's assets worth c_i, and the factor $(1 - \lambda_i^{-1})$ is greater when node i is more highly leveraged. Thus inequality (25) is harder to satisfy, and D is more vulnerable to contagion from i, if large (high asset) nodes in D are more highly leveraged, or if node i is more highly leveraged.
Theorem Implications - A key implication to Theorem 3 is that without substantial node heterogeneity (see Corollary 2 for specific mathematical conditions), contagion with respect to organizational dysfunction will be weak irrespective of the structure of the network induced by the liability matrix (also validated experimentally on real and synthetic data in Section 6). More generally, from Proposition 2, contagion will be weak unless originating node is highly leveraged and has a relative high proportion of obligations to other nodes. Consequently, with respect to node heterogeneity, the following result is immediately obvious.

Corollary 1. *Assume that all nodes i have the same value c for c_i. Under the assumptions of Theorem 1, contagion is weak from any node to any other set of nodes.*

Proof. The result follows from the fact that $\beta_i(1 - \lambda_i^{-1}) < 1$, and the fact that when $c_i = c$, for all i, (25) holds for all i and D. Thus, we have proved Corollary 1. ■

The implication of this corollary is that organizational heterogeneity with respect to resources characterized by c_i's is a necessary condition (though not sufficient) for a cascading service disruption effect to take place. *Since in reality organizations are heterogeneous, cyber-blackouts are possible, though under certain conditions (see Corollary 2)*

Now suppose that $c_1 \geq c_2 \geq ..... \geq c_m$, Since losses are proportional to c_i, a loss to c_1 maximizes the contagion to other nodes. This fact is formalized via the following corollary.

Corollary 2. *If $c_1 \geq c_2 \geq ..... \geq c_m$, then contagion from organizational node 1 to nodes 2,.....,m is weak if $c_2 \geq \beta_1(c_1 - w_1)$ and $c_j \geq (c_{j-1} - w_{j-1})$, $j = 2, ..., m$, strong otherwise. Contagion is impossible if $c_2 - c_m + w_m > \beta_1(c_1 - w_1)$.*

Proof. The result directly follows from (20) and (22). ■

The implications of this corollary are that the lower bounds for c_j ensure that the potential spillovers from other nodes cannot lead to the full set D of nodes into dysfunction *regardless of the liability network topology.* This does not imply that the network structure has no effect on the probability of contagion - it just showcases the fact that in quite a few situations the probability of contagion with respect to organizational dysfunction will be lower than the probability of an organization being rendered dysfunctional due to direct losses (see Section 6 for an experimental validation).
Cyber-Insurance Perspectives- In the context of cyber-insurance, the implications of Proposition 2 carry over, in addition to Theorem 3 and the subsequent corollaries bolstering the future increase in global cyber-insurance market valuation, as risk-averse insurers would not have to worry much about strong contagion effects in selling cyber-insurance policies. In addition, the common knowledge among organizations about inevitable node heterogeneity with respect to monetary assets, will psychologically lead them to invest

in cyber-insurance as well as security enhancing practices due to a certain fear of risk cascading.

With respect to the scale of aggregate risk coverage burden on an insurance company, cyber-blackouts may be quite unlikely if set D is large, which reduces the likelihood of an insurance agency going bankrupt, and this implication holds irrespective of the underlying liability network topology. When D is a small set of heterogeneous organizations, an insurance company is also less likely to be bankrupt, even if some organizations in the set are large-sized and incur large losses. Now as for the case of simultaneous independent direct losses on *all* of the organizations in D which might positively contribute to cyber-blackout probability - in practice, this is a very low probability event for large-sized D.

4.4 Extending the Distribution Space

A drawback with the *Beta* distribution is that the probability of c_i going to zero in the aftermath of a cyber-attack, is zero. This clearly may not be true in practice and we cannot rule out the (potentially futuristic) scenario where the c_i's could be wiped out due to a big cyber-hit - something analogous to a cyber 9/11. In this section, we aim to extend our analysis by accounting for popular loss distributions other than the Beta distribution, that do not suffer from the above-mentioned drawback.

In order to capture the non-positive probability of c_i's going to zero, we propose the following model: Let $X_i^0 \geq 0$ be a *primary loss* (potentially unbounded in size) and let $X_i = (c_i \wedge X_i^0)$ be the resulting loss to c_i for organizational node i - i.e., we truncate the loss to put mass at c_i thereby setting up the way to assign positive probability to c_i going to zero. Assume that the primary losses have a joint distribution of the form:

$$F^0(x_1^0, ..., x_n^0) = \Pi_{1 \leq i \leq n} H^0 \left(\frac{x_i^0}{c_i} \right), \tag{26}$$

where H^0 is a distribution function on the non-negative real line. More specifically, we assume (for now) that the primary losses are i.i.d. and that a given x_i^0 affects every unit of c_i equally. A random variable with distribution function G and density g is said to have an increasing failure rate (IFR) distribution if $\frac{g(x)}{1-G(x)}$ is an increasing function of x. Given the assumption that $Y_i = \frac{X_i^0}{c_i}$ are i.i.d., Y_i's are IFRs. Other popular examples of IFR's are *normal*, *exponential*, and *uniform distributions*; more generally, all *log-concave* distributions. Our model showcases the IFR property common to multiple popular distribution families, and helps us extend results in the previous sub-section to distributions beyond the Beta distribution. We have the following result regarding a non-specific distributional, i.e., IFR-distributed estimate of the cyber-blackout probability.

Theorem 4. *Assume relative primary loss distributions across all organizational nodes are i.i.d. IFR-distributed, and the net worth of every node is initially non-negative. Let D be a non-empty subset of nodes and let $i \notin D$. Then a contagion effect with respect to organizational dysfunction is impossible if*

$$\sum_{j \in D} w_j > w_i \beta_i (\lambda_i - 1), \tag{27}$$

and is weak if

$$\sum_{j \in D} w_j \geq w_i \beta_i \sum_{j \in D} \frac{\lambda_i}{\lambda_j}. \tag{28}$$

Proof. Through relabeling, we can assume that the source node for contagion is $i = 1$ and that the infected nodes are $D = \{2, 3, ..., m\}$. By Proposition 1 we know that contagion is weak from 1 to D if

$$P\left(X_1 > w_1 + \frac{1}{\beta_1} \sum_{2 \leq j \leq m} w_j\right) \leq \Pi_{1 \leq j \leq m} P(X_j > w_j). \tag{29}$$

Since $X_1 = c_1 \wedge X_1^0$, the left-handed side is zero when $w_1 + \frac{1}{\beta_1} \sum_{2 \leq j \leq m} w_j > c_1$. Thus, contagion is impossible if

$$\sum_{2 \leq j \leq m} \frac{w_j}{w_1} > \beta_1(\lambda_1 - 1). \tag{30}$$

Let us therefore assume that $w_1 + \frac{1}{\beta_1} \sum_{2 \leq j \leq m} w_j \leq c_1$. Define the random variables $Y_i = \frac{X_i^0}{c_i}$. Then weak contagion from 1 to D holds if

$$P\left(Y_1 > \frac{w_1}{c_1} + \frac{1}{\beta_1 c_1} \sum_{2 \leq j \leq m} w_j\right) \leq \Pi_{1 \leq j \leq m} P\left(X_j > \frac{w_j}{c_j}\right), \tag{31}$$

where the latter holds from the assumption that Y_i are i.i.d. By assumption that Y_1 is IFR, hence we have from [28]

$$P(Y_1 > s + t | Y_1 > s) \leq P(Y_1 > t), \forall s, t \geq 0.$$

It follows that

$$P\left(Y_1 > \sum_{1 \leq k \leq m} \frac{w_k}{c_k}\right) \leq \Pi_{1 \leq j \leq m} P\left(X_j > \frac{w_j}{c_j}\right) \tag{32}$$

Together with (31) it shows that contagion from 1 to D is weak provided that

$$P\left(Y_1 > \frac{w_1}{c_1} + \frac{1}{\beta_1 c_1} \sum_{2 \leq j \leq m} w_j\right) \leq P\left(Y_1 > \sum_{1 \leq k \leq m} \frac{w_k}{c_k}\right). \tag{33}$$

This clearly holds if

$$\frac{w_1}{c_1} + \frac{1}{\beta_1 c_1} \sum_{2 \leq j \leq m} w_j \geq \sum_{1 \leq k \leq m} \frac{w_k}{c_k}, \tag{34}$$

which is equivalent to

$$\frac{1}{\beta c_1} \sum_{2 \leq j \leq m} w_j \geq \sum_{2 \leq j \leq m} \frac{w_j}{c_j} = \sum_{2 \leq j \leq m} \lambda_j^{-1}. \tag{35}$$

Since $c_1 = \lambda_1 w_1$, we can re-write (35) as

$$\sum_{2 \leq j \leq m} \frac{w_j}{w_1} \geq \beta \lambda_1 \sum_{2 \leq j \leq m} \lambda_j^{-1}. \tag{36}$$

We have therefore shown that if contagion from 1 to $D = \{2, 3, ..., m\}$ is possible at all, then (36) is a sufficient condition for weak contagion with respect to service dysfunctionality. From (36) we see that a simple sufficient condition for weak contagion is $c_j \geq \beta_1 c_1$, $j = 2, ..., m$, and the condition $\sum_{j=2}^m w_j > \beta_1(c_1 - w_1)$ make contagion impossible. Thus, we have proved Theorem 4. ■

Theorem Intuition and Implications - We have the following very powerful system implication as a result of Theorem 4 and Corollary 2, given a single node i (that got hit by a cyber-attack) and an organization set D - *the conditions for weak contagion and the impossibility of contagion with respect to organizational service dysfunction is the same irrespective of the loss distributions and the underlying network topology, as long as the distributions satisfy the general IFR property.* Thus, in a sense the specificity of loss distributions is "irrelevant" to the conditions necessary for a cyber-blackout. The intuition is similar to that of Theorem 3. With respect to node heterogeneity, the following result is immediately obvious from Theorem 4.

Corollary 3. *Assume that all nodes i have the same value c for c_i. Under the assumptions of Theorem 3, contagion is weak from any node to any other set of nodes.*

Proof. It is evident upon writing (36) as

$$\frac{\sum_{j\in D} c_j \lambda_j^{-1}}{\sum_{j\in D} \lambda_j^{-1}} \geq \beta_i c_i.$$

Hence we have proved Corollary 3. ■

Cyber-Insurance Perspective - With respect to cyber-insurance, the implications of Theorem 4 are the same as those from Theorem 3.

Non i.i.d. Primary Losses - In the beginning of this section, we had assumed that primary losses across organizational nodes are i.i.d. However, this assumption is conservative in practice. Here, we provide the conditions for weak contagion for specific but practical loss variables characterized by a Pareto-like or a heavy-tailed densities of the form $P(X_i > x) \approx ax^{-\mu}$ for some positive constants a and μ. First, we generate dependent random variables from independent random variables via a standard statistical procedure as follows: let $Y_1, ..., Y_m$ be independent random variables, each distributed as t_ν - the Student t distribution with $\nu > 2$ degrees of freedom. Let $\hat{Y_1}, ...\hat{Y_m}$ have a standard multivariate Student t distribution with t_ν marginals. Clearly, $\hat{Y_j}$'s are uncorrelated but not independent. In order to make losses positive, we set $\tilde{X_j} = \tilde{Y_j}^2$, for each j, where $\tilde{X_j}$ has a Pareto-like tail.

Proposition 5. *With dependent primary losses, $\tilde{X_i}$,*

$$P(\tilde{X_i} > \sum_{j=1}^{m} w_j) \leq P(\tilde{X_j} > w_j,\ j = 1, ..., m),$$

for all $w_j \geq 0,\ j = 1, 2, ..., m$.

Proof. The proof follows via a direct application of Bound II for the F distribution (see [29]). ■.

The proposition implies that even with heavy-tailed losses, we may find that service dysfunction of a set of nodes through contagion originating from a single organizational node is less likely than service dysfunction via direct losses to individual nodes, if the losses are dependent.

5 Expanding Attack Source and Target Sets

In the previous section, we studied the impact of the dysfunctionality of a single organizational node on another *target set* D of organizational nodes. In this section, we study

the impact of (multiple) successful cyber-attacks on the *entire organizational network.* More specifically, we model our goal as an estimate of the effect of the underlying liability network on the *net losses* in the overall system due to (simultaneous) successful cyber-attacks on c_i's of different organizational nodes i. In this regard, we first need to form a measure of the *total systemic impact* of loss due to cyber-attack. In this work, we shall take the systemic impact of a loss to be the total loss in value summed over all organizational nodes in the network. Given a loss realization $\vec{x}$, the total reduction in resources (assets) across all nodes in the network is

$$\sum_i x_i + S(\vec{x});\ S(\vec{x}) = \sum_i (\bar{p}_i - p_i(\vec{x})). \tag{37}$$

The term $\sum_i x_i$ is the direct loss in value from reductions in liability payments to the i's from their external network environment. The term $S(\vec{x})$ is the indirect loss in value from reductions in liability payments by the nodes to other nodes as well to themselves (due to self-liability). An overall measure of the riskiness of the network system is the expected loss in value, L, given by

$$L = \int (\sum_i x_i + S(\vec{x}))dF(\vec{x}). \tag{38}$$

The question we wish to examine is what proportion of these losses can be attributed to network connections between organizations?

5.1 Examination Setup

Let $\vec{x}$ be a loss value (instance) due to a cyber-attack, and correspondingly let $D = D(\vec{x})$ be the set of nodes that goes dysfunctional given $\vec{x}$. Under our assumptions, this set is unique because the clearing vector is unique. For notational simplicity we suppress $\vec{x}$ in the ensuing discussion. As in the proof of Proposition 4.1, define the shortage in liability payments at organizational node i to be $s_i = \bar{p}_i - p_i$, where $\vec{p}$ is the clearing vector. By definition of D, we have

$$s_i = \begin{cases} > 0,\ \forall i \in D \\ = 0,\ \forall i \notin D \end{cases}$$

Also as in part of Proposition 4.1, let A_D be the $|D|\times|D|$ matrix obtained by restricting the relative liabilities matrix A to D, and let I_D be the $|D| \times |D|$ identity matrix. Similarly let $\vec{s}_D$ be the vector of shortages s_i corresponding to the nodes in D, let $\vec{w}_d$ be the corresponding net worth vector defined in (1), and let $\vec{x}_D$ be the corresponding vector of losses. The clearing condition in (3) implies the following equation, provided $s_i < \bar{p}_i$ (the condition that the net worth of any node is positive), for all i:

$$\vec{s}_D A_D - (\vec{w}_D - x_D) = \vec{s}_D. \tag{39}$$

Recall that A_D is substochastic, and by assumption, there exists a chain of obligations from any given node k to a node having strictly positive obligations to the itself. It follows that $\lim_{k\to\infty} A_D^k = 0_D$, hence $I_D - A_D$ is invertible and

$$[I_D - A_D]^{-1} = I_D + A_D + A_D^2 + ... \tag{40}$$

From (39) and (40), we conclude that

$$\vec{s}_D = (\vec{x}_D - w_D)[I_D + A_D + A_D^2 + ...]. \tag{41}$$

Given a loss instance $\vec{x}$ with resulting dysfunctional organization set $D = D(\vec{x})$, define the vector $u(\vec{x}) \in \mathrm{R}_+^n$ such that

$$u_D(\vec{x}) = [I_D + A_D + A_D^2 + ...] \cdot 1_D,\ u_i(\vec{x}) = 0,\ \forall i \notin D. \tag{42}$$

Combining (37), (41), and (42) shows that the total losses for a given $\vec{x}$ can be expressed as

$$L(\vec{x}) = \sum_i (x_i \wedge w_i) + \sum_i (x_i - w_i) u_i(\vec{x}). \tag{43}$$

The first term represents the direct losses to remaining resources at each organizational node, and the second term represents the total shortage summed over all the nodes. The right side becomes an upper bound on $L(x)$ if $s_i = \bar{p}_i$ for some $i \in D(\vec{x})$. We call the coefficient $u_i = u_i(\vec{x})$ the *depth* of organizational node i in $D = D(x)$. The rationale for this terminology is as follows. Consider a Markov chain on D with transition matrix A_D. For each $i \in D$, u_i is the expected number of periods before exiting D, starting from node i. Expression (42) shows that *node depths measure the amplification of losses due to interconnections among nodes in the dysfunctional set.* We note here that the concept of node depth is dual to the notion of eigenvector centrality (or eigenvector-driven centrality measures) [30]. To see the connection, let us restart the Markov chain uniformly in D whenever it exits D. This modified chain has an ergodic distribution proportional to $1_D \cdot [I_D + A_D + A_D^2 + ...]$ and its ergodic distribution measures the centrality of the nodes in D. It then follows that node depth with respect to A_D corresponds to centrality with respect to the transpose of A_D.

We can now bound the magnitude of the node depths in the dysfunctional set. We first define a set D of nodes to be α-*cohesive* if every node in D has at least α of its liabilities to other nodes in D, i.e., $\sum_{j \in D} a_{ij} \geq \alpha$, for every $i \in D$ [31]. The *cohesiveness* of D is the maximum α, which we denote by α_D. As a lower bound for u_i, it follows from (42) it follows that

$$u_i \geq \frac{1}{1 - \alpha_D},\ \forall i \in D. \tag{44}$$

Thus, *the more cohesive the dysfunction set, the greater the depth of the nodes in that set and the greater the amplification of the associated loss.* We can also bound the node depths from above. Recall that β_i is the proportion of i's liability to other nodes in the network. Let $\beta_D = \max\{\beta_i : i \in D\}$. We obtain the upper bound assuming $\beta_D < 1$ as follows:

$$u_i \leq \frac{1}{1 - \beta_D},\ \forall i \in D. \tag{45}$$

The bounds in (44) and (45) depend on the dysfunctional set D, which in turn depends on $\vec{x}$. A uniform upper bound is given by

$$u_i \leq \frac{1}{1 - \beta^+},\ \forall i \in D;\ \beta^+ = \max \beta_i < 1. \tag{46}$$

We are now in a position to compare the expected systemic losses in a given network of interconnections, with the expected losses without such interconnections, in order to gauge the effect of service disruption contagion in a network.

5.2 Comparing Expected Systemic Losses

Consider the following system setting as already discussed in Section 2. We fix a set of n organizational nodes, $N = \{1, 2, ..., N\}$, vectors $\vec{c}$, and $\vec{b}$ as before. Assume that the

net worth w_i of node i is non-negative before a loss due to a cyber-attack is realized, and that liability network interconnections are determined via the $n \times n$ matrix $\bar{P}$. Let us now have another system setting where we eliminate all connections between nodes, i.e., let $\bar{P}^0$ be the $n \times n$ matrix of zeros. Each node i in this setting has resources c_i that are yet to be attack-targeted, and self liabilities, b_i. In order to keep an organization's net worth unchanged, we introduce "fictitious" resources c_i and self liabilities b_i to maintain balance. More specifically, if $c_i - b_i < w_i$, we give i a new class of resources in the resource amount $c_i' = w_i - (c_i - b_i)$. If $c_i - b_i > w_i$, we give i a new class of self liabilities in the amount $b_i' = w_i - (c_i - b_i)$. We assume that the new resources are safe, i.e., they are not subject to cyber-attacks, and that the new liabilities have the same priority as other liabilities. Let $F(x_1, ...x_n)$ be a joint loss distribution that is homogeneous in resources, i.e., $F(x_1, ..., x_n) = G(\frac{x_1}{c_1}, \frac{x_2}{c_2}, ...\frac{x_n}{c_n})$, where G is a symmetric c.d.f. We do not assume that losses across nodes are independent. We say that F is IFR if its marginal distributions are IFR; this is equivalent to saying that the marginals of G are IFR. Let $\bar{L}$ be the expected total losses in the original network and let $\bar{L}^0$ be the expected total losses when the connections are removed. We have the following result relating $\bar{L}$ and $\bar{L}^0$.

Theorem 6. *Let $N(\vec{b}, \vec{c}, \vec{w}, \bar{P})$ be an organizational network system and let N^0 be the analogous system with all the network connections removed. Assume that the loss distribution is homogeneous in resources and IFR. Let $\beta^+ = \max_i \beta_i < 1$, and let $\delta_i = P(X_i \geq w_i)$. Then the ratio of expected losses in N^0 is at most*

$$\frac{\bar{L}}{\bar{L}_0} \leq 1 + \frac{\sum_i \delta_i c_i}{(1-\beta^+)\sum_i c_i}. \tag{47}$$

Proof. By assumption, the marginals of F are IFR distributed. A general property of IFR distributions is that "new is better than used in expectation", i.e.,

$$E[X_i - w_i | X_i \geq w_i] \leq E[X_i], \tag{48}$$

from [28]. It follows that

$$E[(X_i - w_i]^+] \leq P(X_i \geq w_i) E[X_i] = \delta_i E[X_i]. \tag{49}$$

By (43) we know that the total expected losses $\bar{L}$ can be bounded as

$$\bar{L} \leq \sum_i E[X_i \wedge w_i] + E[\sum_i (X_i - w_i) u_i(X)]. \tag{50}$$

From (46) we know that $u_i \leq \frac{1}{1-\beta^+}$ for all i; furthermore we clearly have $X_i - w_i \leq (X_i - w_i)^+$ for all i. Thus,

$$\bar{L} \leq \sum_i E[X_i \wedge w_i] + (1-\beta^+)^{-1} \sum_i E[(X_i - w_i)^+]. \tag{51}$$

From this and (49) it follows that

$$\bar{L} \leq \sum_i E[X_i \wedge w_i] + (1-\beta^+)^{-1} \sum_i \delta_i E[X_i], \tag{52}$$

which reduces to

$$\bar{L} \leq \sum_i E[X_i] + (1-\beta^+)^{-1} \sum_i \delta_i E[X_i]. \tag{53}$$

When the network connections are excised, the expected loss is simply the expected sum of the losses, that is $\bar{L}^0 = \sum_i E[X_i]$. By the assumption of homogeneity in resources we know that $E[X_i] \propto c_i]$ for all i. We conclude from this and (53) that

$$\frac{\bar{L}}{\bar{L}_0} \leq 1 + \frac{\sum_i \delta_i c_i}{(1-\beta^+)\sum_i c_i}.$$

Thus, we have proved Theorem 6. ■

Theorem Implications - The theorem shows that increases in losses due to liability network interconnections will be very small unless β^+ (the maximum proportion of obligations by any node in the network) is close to 1, or the rate at which an organization becomes dysfunctional is high, both of which are quite unlikely in practice. Moreover, the latter statement also holds when the losses across nodes are dependent or correlated, regardless of the network structure.

Cyber-Insurance Perspective - Since the losses due to networked connectivity is primarily amplified due to a high β^+, which in turn implies high dysfunctionality rate of an organization, it is imperative that cyber-insurers impose a strict control policy via their contracts with the organizations to ensure the highest standards of cyber-hygiene from the latter that results in low/moderate values of β^+. This in turn would reduce the probability of a cyber-blackout and also mitigate the chances of cyber-insurers going bankrupt in the process of covering correlated aggregate risk. An intuitively evident insurance policy mechanism in this regard is to premium discriminate between good hygiene and bad hygiene organizations [32]. Such policies have been shown to be market efficient in the economic sense.

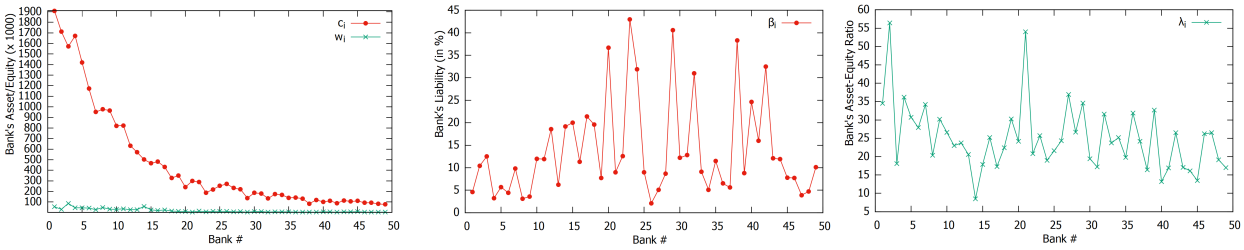

Figure 1: Experimental Parameters for Real-World Data - (a) c_i and w_i values (left), (b) β_i values (middle), and λ_i values (right)

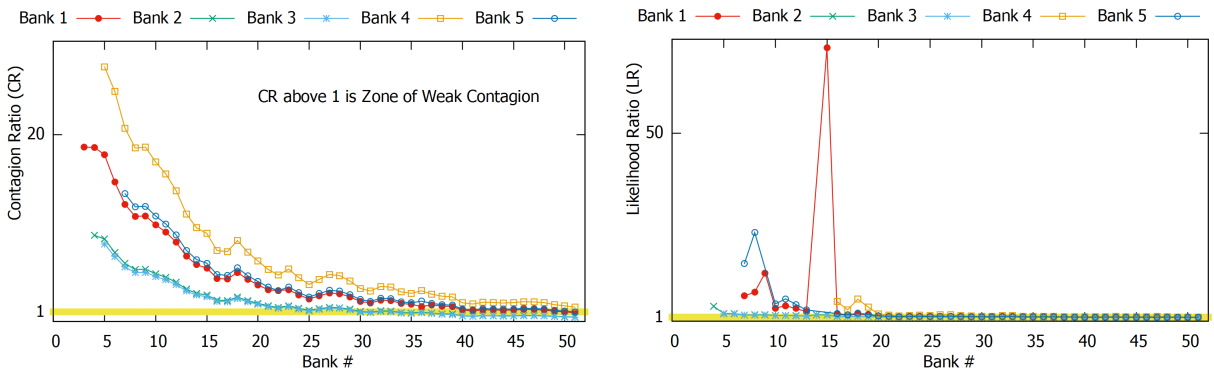

Figure 2: Performance on Real-World Data (a) Contagion Ratio (CR) (left), (b) Likelihood Ratio (LR) (right)

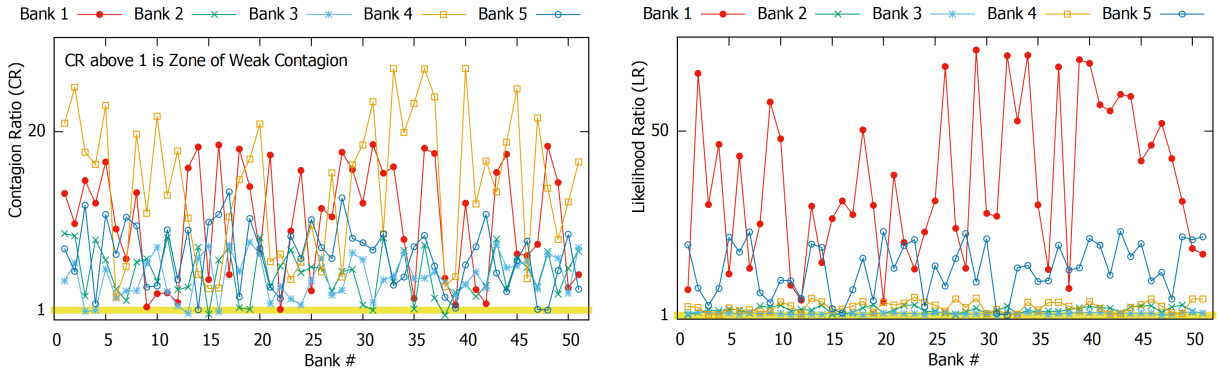

Figure 3: Performance on Instance #1 of Synthetic Data (a) Contagion Ratio (CR) (left), (b) Likelihood Ratio (LR) (right)

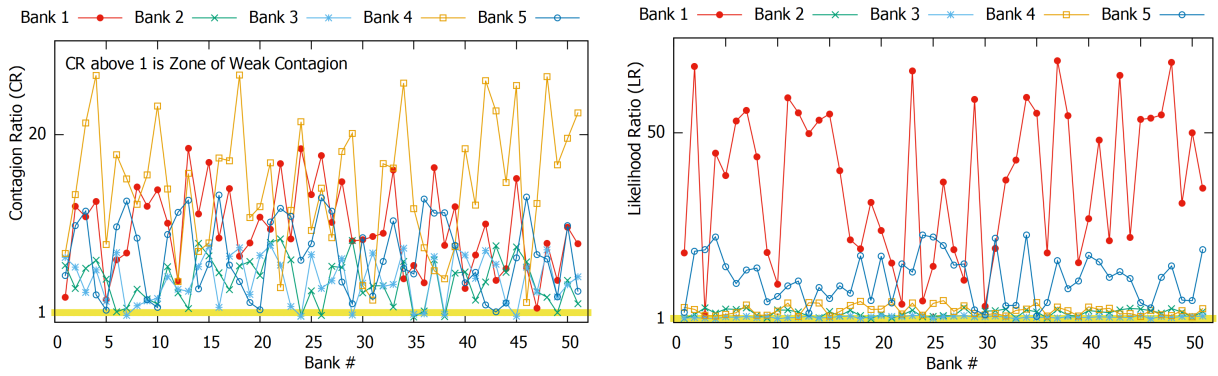

Figure 4: Performance on Instance #2 of Synthetic Data (a) Contagion Ratio (CR) (left), (b) Likelihood Ratio (LR) (right)

6 Experimental Evaluation

Experimenting with multiple real-world data sets related to cyber-attacks and their subsequent impact is an extremely difficult task, as data on cyber-security is really hard to obtain. As a result, in this section, we experiment on both real-world and synthetic banking sector application data obtained post a cyber-attack in the European Union. In this regard, we study the effects of parameters c_i, w_i, λ_i, and β_i on strong and weak contagion phenomena, in turn studying how our theoretical results apply in practice. We also experiment on synthetic data to study the effect of network topology on contagion phenomena.

6.1 Experimental Setup

One of the responsibilities of the European Banking Authority (EBA) is to ensure the orderly functioning and integrity of financial markets and the stability of the banking system in the EU. A primary supervisory tool to conduct such an analysis is via a stability test exercise. The aim of such a test is to assess the resilience of banking institutions to adverse market developments, as well as to contribute to the overall assessment of systemic risk in the EU banking system, where the systemic risk could be due to a cyber-attack. We collected data for a cyber-attack induced stress test done in 2015. *Detailed information on inter-bank exposures needed to calibrate a full network was not publicly available. As a result, as aforementioned, we also generated 50 instances of synthetic random networks between banks in the 2015 data set to study the effect of network topology on the contagion phenomena.*

For the real data set, 90 banks from 21 countries participated in the stress test. For each bank, the EBA reports each bank's total exposure at the dysfunction state to other banks. The EAD measures a bank's total claims on all other banks, so we take this as the size of each bank's in-network assets. Subtracting this value from the total assets gives us c_i. For w_i (see Figure 1(a)), we use the equity values reported by the EBA, which then allows us to calculate $\lambda_i = \frac{c_i}{w_i}$ (see Figure 1(c)). The only remaining parameter we need is β_i, the fraction of a bank's liabilities owed to other banks. This information is not included in the EBA summary, nor is it consistently reported by the banks in their statements. As a rough indication, we assume that each bank's in-network liabilities equal its in-network assets[3]. This gives us $\beta_i = \frac{EAD}{assets-equity}$ (see Figure 1(b)). Some of the smallest banks have a problematic data, so as a simple rule we omit the ten smallest. We also omit any countries with only a single participating bank. This leaves us with 76 banks, out of which we work with 50 largest banks. For synthetic data sets, we estimate the parameters c_i, w_i, λ_i, and β_i in the same manner as for our real-world data set.

We examine the potential for contagion from the failure of the five largest banks (Bank #'s 1-5 in the figures). Taking each of these in turn as the triggering bank, we then take the dysfunctional set D to be consecutive pairs of banks, e.g., the first dysfunctional set under Bank #1 is Bank numbers 2 and 3, the next dysfunctional set consist of Bank numbers 3 and 4, and so on. As peformance metrics we study 'Contagion Ratio' (CR) and 'Likelihood Ratio' (LR), where we define CR to be the ratio of the LHS of inequality (17) to the RHS of the inequality. We term CR as 'weak' if it is greater than 1. We define LR to be the relative probability of organizational dysfunction through independent direct cyber-shocks and through contagion, calculated as the ratio of the RHS of (18) to LHS.

6.2 Experimental Results

From Figures 2(a)-4(a), we observe that CR is weak for most organizations, validating our theory that cyber-blackouts through strong contagion effects are less likely. CR fails to be weak only when banking organizations in the dysfunction set D are much smaller (in monetary worth) than the triggering bank. Moreover, the value of CR reported for each bank shows how much β_i would have to be to reverse the direction of inequality (17). In this sense the plots in Figure 2(a) are robust to the estimated values of β_i. Expanding the size of set D makes contagion weaker because of the relative magnitudes of w_i and λ_i^{-1}. High values of LR indicate the dominance of the probability of organizational node dysfunction through independent shocks over node dysfunction through contagion. Our plots show that the LR is mostly greater than 1, validating our theory that contagion does not play a major role in organizational dysfunction in the event of a cyber-attack. From Figures 3 and 4 (2 of the 50 random synthetic instances), we observe that network topology does not have a significant role in shaping the contagion phenomenon, i.e., majority of organizations are in the weak contagion zone. However, the CR ratios differ from topology to topology as evident in differences in the plot structure between Figure 2 and Figures 3-4. Even we do not have information on the organizational liability topology of our real-world data, it is evident there is a structure to that topology compared to those characterizing synthetic data.

[3]Based on Federal Reserve Release, the average value of β_i for commercial banks in the USA is about 3%, so our estimates for European banks would appear to be conservative.

7 Related Work

In this section, we cite works most related to ours in this paper. However, we would like to emphasize upfront that a rigorous analysis of cyber-blackout phenomena in a network is absent in literature for cyber-insurance or network risk management settings, and our efforts here in this direction are completely new to the best of knowledge. We structure this section in two parts that form a tangential relationship to our work in this paper: (a) cyber-insurance market success, and (b) risk estimation in network contagion settings.

7.1 Success of Cyber-Insurance Markets

In this work we investigated worst case scenarios for a cyber-insurer to cover aggregate cyber-risks. However, a pre-cursor is to have working successful markets in the first place. To this end, recent research works on cyber-insurance [33][18][34] have mathematically shown the existence of economically inefficient insurance markets. Intuitively, an efficient market is one where all stakeholders (market elements) mutually satisfy their interests. These works state that cyber-insurance satisfies every stakeholder apart from the regulatory agency (e.g., government), and sometimes the cyber-insurer itself. The regulatory agency is unsatisfied as overall network robustness is sub-optimal due to network users not optimally investing in self-defense mechanisms, whereas a cyber-insurer is unsatisfied due to it potentially making zero expected profit at times. Lelarge et al. in [18] recommended the use of fines and rebates on cyber-insurance contracts to make each user invest optimally in self-defense and make the network optimally robust. However, their work neither mathematically proves the effectiveness of premiums and rebates in making network users invest optimally, nor does it guarantee the strict positiveness of insurer profits at all times. In a recent work [35][36], the authors overcome the drawbacks of the mentioned existing works, and propose ways to form provably efficient monopolistic cyber-insurance markets by satisfying market stakeholders, including a risk-averse cyber-insurer, in environments of interdependent risk. In addition, recent major successful cyber-attacks on large commercial organizations have significantly increased board-level concerns to maintain business reputation amongst clients, and subsequently accelerated the adoption of cyber-insurance products in the industry.

Drawbacks - These works do not investigate aggregation risk likelihoods for a cyber-insurer in a networked setting - a prime determinant for the expansion of the insurance industry.

7.2 Estimation in Attack Spread Settings

In Section III, we emphasized that evaluating $F()$ actually involves mathematically capturing the spread of the infection (attack) vector (e.g., a virus, bot), and is not the focus of this paper. Here, we are only interested in the process of the spread of "organizational dysfunctionality" due to cyber-attacks. The interested reader is referred to [18][19][20] to get insights on statistical mean field models to mathematically evaluate $F()$. To the best of our knowledge, no work exists on the spread of "organizational dysfunctionality" due to cyber-attacks as we imply in the paper. In terms of the process of the spread of attacks in networks, a related literature has directly originated from the study of cascades. Various models have been developed in the computer science and network science literatures, including the widely-used threshold models [37] and percolation models [38][39][40][41][42][43][44][45]. A few works have applied these ideas to various economic settings, including [46] and [47] in the context of economic fluctuations; [31] in the context of contagion of different types of strategies in coordination games; and more recently,

[48] and [49] in the context of spread of an epidemic-like financial contagion, where the seminal papers of [50] and [51] developed some of the first formal models of contagion over financial networks.
Drawbacks - Attack propagation does not imply service disruption. To this end, none of the above works investigate the propagation of service dysfunctionality in a network.

8 Discussion and Summary

Our work in this paper has looked into the future of cyber-insurance coverage for the inter-dependent IT service sector, with respect to quantifying the probability of a cyber-blackout. However, the cyber-blackout scenario though quite relevant for current general cyber-insurance scenarios (energy, property, marine, aviation, etc.), is not considered, i.e., excluded, while selling insurance policies at present, simply due to insurance agencies being considerably risk-averse on a ruin event arising for correlated and aggregate risk. In future, with respect to blackout events, the insurance industry will likely evolve to address quantifiable cyber-risk large enough to produce a market for it but small enough to be manageable. Re-insurance is a possible option to cover large-valued risks due to a blackout event, but for any sorts of reinsurance the risks of the individual policies must be aggregated. In this regard, the regulations affecting the risk of each company would not be treated differently than any other risk that differs across companies / individual policies. In the case of big service providing companies (e.g., Google), the latter currently do not burden themselves with the risk of those using their services. In future, this pattern is likely to continue unless legally mandated or as part of some special service offering. In that regard, we foresee companies like Google to essentially just become the insurer themselves.
Summary - In this paper, we studied the general question: *is a cyber-blackout in a service organizational network likely?* More specifically, we estimated the probability that all or a major subset of nodes in the network become dysfunctional to provide service in the event of a cyber-attack, a situation which we define as a *cyber-blackout*. The motivation for our research stems from the fact that service liability interconnections among networked IT-driven service organizations create potential channels for cascading service disruptions due to modern cybercrimes such as DDoS, APT, and ransomware attacks, and cause a bankruptcy-scare effect amongst cyber-insurers via covering aggregate cyber-risk.

As part of our research contributions, we first designed a graph-based model of service obligations, *GSOM*, between organizations in a service chain network. In the event of a cyber-attack, given the values of losses at the nodes in the network, GSOM computes the vector of service valuations that clears the network, and identifies the nodes in the chain that are dysfunctional to provide service. Using GSOM, we then analyzed (i) how likely it is that a given set of target organizations will become dysfunctional due to contagion from a single source organization, as compared to the likelihood that they become dysfunctional from direct losses to their own service-related assets that does not require dependency on other nodes?, and (ii) how much does the underlying network of service dependencies contribute to the increase in the probability of dysfunction of target nodes and corresponding expected value of losses, compared to a situation when there are no network links. As a surprising result, we showed that the loss probability is larger in the absence of network connectivity than that in the presence of network connectivity, implying that simple network spillover effects have a limited impact (except under specific conditions) with respect to service obligations between organizations. We also showed that total additional losses due to network spillover effects are surprisingly small under a wide range of joint distributions for plausible values of model parameters.

Finally, we expanded the set of attack sources from a single node to multiple nodes, and studied the negative impact of simultaneous attacks on the entire network. We again showed that the increase in losses due to network interconnections are very small (except under a certain less likely condition), independent of the network structure and under general assumptions about the joint loss distribution. The primary rationale behind our results are attributed to degrees of heterogeneity in wealth base among organizations, and Increasing Failure Rate (IFR) property of loss distributions.

References

[1] R. Betterley, "Cyber/privacy insurance market syurvey-2015," *The Betterley Report*, 2015.

[2] P. Millaire, "3 reasons why the insurance industry will never be the same after the mirai ddos attack," in *Symantec Connect*, 2016.

[3] L. Eisenberg and T. H. Noe, "Systemic risk in financial systems," *Management Science*, vol. 47, no. 2, pp. 236–249, 2001.

[4] "Managing cyber insurance accumulation risk," *Cambridge Center for Risk Studies*, 2016.

[5] "UK hospital meltdown after ransomware worm uses NSA vuln to raid IT," *The Register, UK*, 2017. `https://www.theregister.co.uk/2017/05/12/nhs_hospital_shut_down_due_to_cyber_attack/`

[6] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired Magazine*, 2018. `https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/`

[7] E. Ronen, A. Shamir, A.O. Weingarten, and C. OFlynn, "IoT goes nuclear: Creating a ZigBee chain reaction.," *In Security and Privacy (SP), 2017 IEEE Symposium on (pp. 195-212). IEEE.*, pp. 195–212, 2017.

[8] J.cKrystlik, "With gdpr, preparation is everything," *Computer Fraud & Security*, vol. 2017, no. 6, pp. 5–8, 2017.

[9] Z. Whittaker, "Mirai botnet attack hits thousands of home routers, throwing users offline," *ZDNet, Nov*, vol. 29, 2016.

[10] A. Greenberg, "How an entire nation became russia's test lab for cyberwar," *WIRED*, vol. 20, p. 2017, 2017.

[11] K. Chinthapalli, "The hackers holding hospitals to ransom," *BMJ*, vol. 357, p. j2214, 2017.

[12] V. Morabito, "The security of blockchain systems," in *Business Innovation Through Blockchain*. Springer, 2017, pp. 61–78.

[13] J. Robertson and M. Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," in *Bloomberg Businessweek*. 2018, Accessed: 05-October-2018.

[14] S. Grobman, "When nation-states hack the private sector for intellectual property," in *The Hill*. 2018, Accessed: 05-October-2018.

[15] Wikipedia. Contributors, "Sony Pictures hack," in *Wikipedia*. 2014, Accessed: 05-October-2018.

[16] Wikipedia. Contributors, "2007 cyberattacks on Estonia," in *Wikipedia*. 2007, Accessed: 05-October-2018.

[17] T. Tracy , "Apple Stock: Analyzing 5 Key Customers (AAPL)," in *Investopedia*. 2016, Accessed: 05-October-2018.

https://www.investopedia.com/articles/insights/050116/apple-stock-analyzing-5-key-customers-aapl.asp

[18] M. Lelarge and J. Bolot, "Economic incentives to increase security in the internet: The case for insurance," in *IEEE INFOCOM*, 2009.

[19] J. Lorenz, S. Battiston, and F. Schweitzer, "Systemic risk in a unifying framework for cascading processes on networks," *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 71, no. 4, pp. 441–460, 2009.

[20] A. Ganesh, L. Massoulié, and D. Towsley, "The effect of network topology on the spread of epidemics," in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, vol. 2. IEEE, 2005, pp. 1455–1466.

[21] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Networks formed from interdependent networks," in *Nature physics*, vol. 2, no. 1, Nature Publishing Group, 2012, pp. 40.

[22] F. J. Fabozzi and H. M. Markowitz, *The theory and practice of investment management*. John Wiley & Sons, 2002, vol. 118.

[23] B. Wootton, *Who's Using Amazon Web Services?*. Contingo, 2017. `https://www.contino.io/insights/whos-using-aws`

[24] AWS Sales, *Case Studies & Customer Success - Amazon Web Services (AWS)*. Amazon 2018. `https://aws.amazon.com/solutions/case-studies/`

[25] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Security pricing as enabler of cyber-insurance a first look at differentiated pricing markets," *IEEE Transactions on Dependable and Secure Computing*, 2017.

[26] Symantec, "Attackers target both large and small businesses," in *Symantec Business*, 2016.

[27] N. L. Johnson, S. Kotz, and N. Balakrishnan, "Continuous univariate distributions, vol. 2 of wiley series in probability and mathematical statistics: applied probability and statistics," 1995.

[28] R. Barlow and F.Proschan, *Statistical Theory of Reliability and Life-Testing*. John Wiley and Sons Inc., 1975.

[29] A. W. Marshall and I. Olkin, "Majorization in multivariate distributions," *The Annals of Statistics*, pp. 1189–1200, 1974.

[30] M. Newman, *Networks: an introduction*. Oxford university press, 2010.

[31] S. Morris, "Contagion," *The Review of Economic Studies*, vol. 67, no. 1, pp. 57–78, 2000.

[32] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security? a market analysis," in *INFOCOM, 2014 Proceedings IEEE*. IEEE, 2014, pp. 235–243.

[33] A. Hoffman, "Internalizing externalities of loss prevention through insurance monopoly," *Geneva Risk and Insurance Review*, vol. 32, 2007.

[34] N.Shetty, G.Schwarz, M.Feleghyazi, and J.Walrand, "Competitive cyber-insurance and internet security," in *WEIS*, 2009.

[35] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security: A market analysis," *INFOCOM, 2014 Proceedings IEEE*, pp. 235–243, 2014.

[36] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Improving Cyber-Security via Profitable Insurance Markets," *ACM SIGMETRICS Performance Evaluation Review*, vol. 45, no. 4, pp. 7–15, 2018.

[37] M. Granovetter, "Threshold models of collective behavior," *American journal of sociology*, vol. 83, no. 6, pp. 1420–1443, 1978.

[38] R. J. La, "Interdependent security with strategic agents and cascades of infection", *IEEE/ACM Transactions on Networking (TON)*, vol. 24, no. 3, pp. 1378–1391, 2016.

[39] R. J. La, "Influence of clustering on cascading failures in interdependent systems", *IEEE Transactions on Network Science and Engineering*, 2018.

[40] R. J. La, "Cascading failures in interdependent systems: impact of degree variability and dependence", *IEEE Transactions on Network Science and Engineering*, vol. 5, no. 2, pp. 127–140, 2018.

[41] D. J. Watts, "A simple model of global cascades on random networks," *Proceedings of the National Academy of Sciences*, vol. 99, no. 9, pp. 5766–5771, 2002.

[42] M. Molloy and B. Reed, "The size of the giant component of a random graph with a given degree sequence," *Combinatorics, probability and computing*, vol. 7, no. 3, pp. 295–305, 1998.

[43] ——, "A critical point for random graphs with a given degree sequence," *Random structures & algorithms*, vol. 6, no. 2-3, pp. 161–180, 1995.

[44] M. E. Newman, S. H. Strogatz, and D. J. Watts, "Random graphs with arbitrary degree distributions and their applications," *Physical review E*, vol. 64, no. 2, p. 026118, 2001.

[45] F. Chung and L. Lu, "Connected components in random graphs with given expected degree sequences," *Annals of combinatorics*, vol. 6, no. 2, pp. 125–145, 2002.

[46] S. N. Durlauf, "Nonergodic economic growth," *The Review of Economic Studies*, vol. 60, no. 2, pp. 349–366, 1993.

[47] P. Bak, K. Chen, J. Scheinkman, and M. Woodford, "Aggregate fluctuations from independent sectoral shocks: self-organized criticality in a model of production and inventory dynamics," *Ricerche Economiche*, vol. 47, no. 1, pp. 3–30, 1993.

[48] P. Gai and S. Kapadia, "Contagion in financial networks," in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*. The Royal Society, 2010, p. rspa20090410.

[49] L. Blume, D. Easley, J. Kleinberg, R. Kleinberg, and É. Tardos, "Which networks are least susceptible to cascading failures?" in *Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on*. IEEE, 2011, pp. 393–402.

[50] F. Allen and D. Gale, "Financial contagion," *Journal of political economy*, vol. 108, no. 1, pp. 1–33, 2000.

[51] X. Freixas, B. M. Parigi, and J.-C. Rochet, "Systemic risk, interbank relations, and liquidity provision by the central bank," *Journal of money, credit and banking*, pp. 611–638, 2000.